



# LOAN DOCUMENT

<p style="font-size: 24pt; font-weight: bold;">AD-A265 284</p>  <p style="writing-mode: vertical-rl; transform: rotate(180deg); font-size: 10pt;">DTIC ACCESSION NUMBER</p>	<p style="text-align: center;">PHOTOGRAPH THIS SHEET</p> <div style="border: 1px solid black; height: 80px; margin: 5px;"></div> <p style="text-align: center;">LEVEL</p>	<div style="border: 1px solid black; height: 80px; margin: 5px; display: flex; align-items: center; justify-content: center;"> <span style="font-size: 48pt; border: 1px solid black; border-radius: 50%; padding: 10px;">1</span> </div> <p style="text-align: right;">INVENTORY</p> <p style="font-size: 18pt; margin-top: 10px;">Architecture Master Plan Study Concept Paper Security Vol. 38</p> <p style="text-align: center;">DOCUMENT IDENTIFICATION Jul 89</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px; text-align: center;"> <p><del>DISTRIBUTION STATEMENT A</del></p> <p>Approved for public release Distribution Unlimited</p> </div> <p style="text-align: center;">DISTRIBUTION STATEMENT</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px; text-align: center;"> <p style="font-size: 24pt; font-weight: bold;">DTIC ELECTE MAY 28 1993</p> <p style="font-size: 48pt; font-weight: bold;">S C D</p> </div> <p style="text-align: center;">DATE ACCESSIONED</p> <div style="border: 1px solid black; height: 100px; margin-top: 10px;"></div> <p style="text-align: center;">DATE RETURNED</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px; text-align: center;"> <p style="font-size: 24pt; font-weight: bold;">93-12063</p>  </div> <p style="text-align: center;">REGISTERED OR CERTIFIED NUMBER</p>													
<p style="font-size: 10pt;">ACCESSION FOR</p> <table style="width: 100%; font-size: 8pt;"> <tr> <td>NTIS</td> <td>GRAB</td> <td rowspan="4" style="text-align: center; vertical-align: middle;"> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </td> </tr> <tr> <td>DTIC</td> <td>TRAC</td> </tr> <tr> <td>UNANNOUNCED</td> <td></td> </tr> <tr> <td>JUSTIFICATION</td> <td></td> </tr> </table> <p style="margin-top: 10px;">BY <u>Per LK</u></p> <p style="font-size: 10pt;">DISTRIBUTION/</p> <p style="font-size: 10pt;">AVAILABILITY CODES</p> <table style="width: 100%; font-size: 8pt;"> <tr> <td style="width: 30%;">DISTRIBUTION</td> <td style="width: 70%;">AVAILABILITY AND/OR SPECIAL</td> </tr> <tr> <td style="height: 60px; vertical-align: bottom; font-size: 24pt;">A-1</td> <td></td> </tr> </table>	NTIS	GRAB	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	DTIC	TRAC	UNANNOUNCED		JUSTIFICATION		DISTRIBUTION	AVAILABILITY AND/OR SPECIAL	A-1		<p style="text-align: center;">DISTRIBUTION STAMP</p> <div style="border: 1px solid black; height: 100px; margin-top: 10px;"></div> <p style="text-align: center;">DATE RECEIVED IN DTIC</p>	
NTIS	GRAB	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>													
DTIC	TRAC														
UNANNOUNCED															
JUSTIFICATION															
DISTRIBUTION	AVAILABILITY AND/OR SPECIAL														
A-1															
<p>PHOTOGRAPH THIS SHEET AND RETURN TO DTIC-FDAC</p>															

HANDLE WITH CARE

- 38 -

**UNITED STATES  
DEPARTMENT OF DEFENSE  
Computer-aided Acquisition &  
Logistic Support (CALS)**

**July 1989**

**OSD CALS  
Architecture Master Plan Study**

**CONCEPT PAPER**

**SECURITY**

**Prepared by**

**U.S. Department of Transportation  
Research and Special Programs Administration  
Transportation Systems Center  
Cambridge, MA 02142**

## *EXECUTIVE SUMMARY*

Developing and executing a well-thought-out security policy is critical to the success of CALS. Without appropriate security measures, the integration of technology, organizations, functions, and data envisioned as Phase II CALS can not occur. Therefore security must be viewed as a critical "disabling technology" and must be satisfied to expedite integration.

Expanding the computing base in terms of both functionality and scope is the most significant factor influencing CALS security requirements. The new functionality that needs to be protected includes database management systems, communications software, network software, network configurations, and remote peripheral equipment. Growth in the number of systems and users linked together constitutes the second aspect of this expansion that places new demands upon security.

Although current DoD security practices are adequate for CALS Phase I digital exchange initiatives, there are numerous unsatisfied security requirements facing a shared-data environment envisioned as CALS Phase II. Even though satisfying all security requirements is necessary for a successful CALS, requirements that are unique to CALS are of primary interest from a CALS policy perspective. Therefore OSD needs to incorporate activities of other organizations in their plans, and only undertake activities that will satisfy CALS unique requirements.

CALS unique security requirements are both technical and administrative in nature, involving data security, system security, and network security. Classification categories and procedures for business sensitive information, and protection strategies to prevent the unauthorized aggregation and disclosure of information are the primary data security requirements facing CALS. CALS system security requirements include certification and accreditation guidelines, a CALS security risk assessment, and procedures to administer data accountability in a Phase II shared-data environment. Network security may be the most problematic area for CALS. Requirements include a data encryption scheme and procedures to manage and administer the distribution and use of keys.

OSD needs to initiate those prerequisite activities that will alert the Office to specific "disablers" and enable the Office to provide guidance on security to the Services and commercial vendors. These activities include:

- Define a CALS security concept of operations;
- Develop a protection philosophy and identify appropriate risk management mechanisms;
- Initiate accreditation planning; and
- Develop implementation strategies.

# CONTENTS

Executive Summary	i
Section 1 - Introduction	1
Section 2 - Security within DoD	3
Section 3 - Security within CALS	9
Section 4 - Recommendations	15

# SECTION 1. INTRODUCTION

## 1.1 Report Purpose and Structure

This paper defines the high-level security requirements facing the CALS initiative and suggests a strategic approach to meet these requirements. To this end, the paper also promotes a common understanding of computer security and security issues within a DoD/CALS environment.

In addition to this introductory section, the report devotes a section to each of the following topics:

- **Section 2 - Security within the DoD** discusses current DoD policies and practices, and outlines the direction of emerging security procedures.
- **Section 3 - Security within CALS** examines emerging security needs and defines high-level requirements for CALS.
- **Section 4 - Recommendations** describes a strategic approach to CALS security requirements and defines an initial set of tasks.

## 1.2 Background

Three distinct elements are within the scope of security. As pictured in Figure 1, these elements are system resources security, security procedures, and security threats.

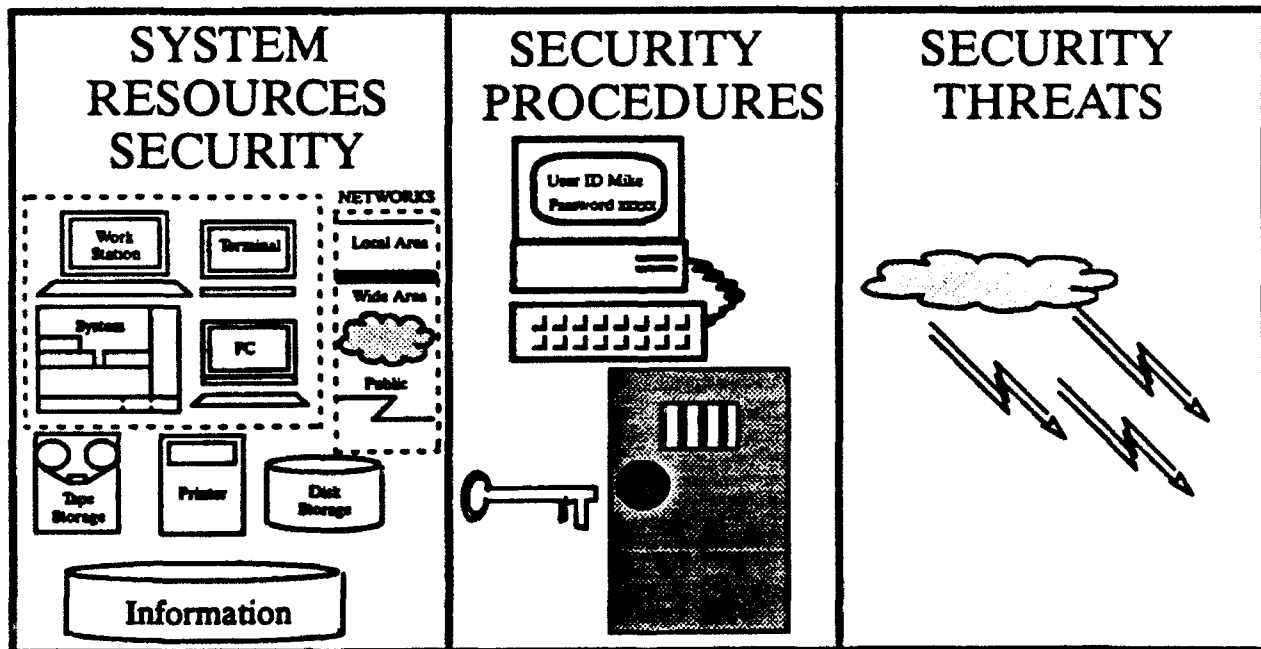


FIGURE 1. Computer Security Scope

**System Resources Security** concerns computer systems and the information they maintain. System resources include hardware, firmware, and software for stand-alone systems and also network system components such as transmission signals and lines, network/communications software, and hardware.

**Security procedures** include concepts, techniques, and measures used to protect computer systems and the information they maintain. Security procedures reflect regulations, directives, and circulars and are either physical, administrative, or technical in nature.

**Security threats** are situations that menace system resources, – particularly the information they maintain. Threats can be grouped in two categories: human and environmental. Human threats can be intentional and unintentional. Environmental threats are either fabricated or natural.

Given this context, the broad goal of any security policy is to neutralize or mitigate security threats using cost-effective security procedures, thereby protecting system resources. Computer security procedures must therefore satisfy the following three objectives:

- Prevent unauthorized use or disclosure of data or other system resources;
- Assure the integrity of system resources, including data, applications, and equipment: and
- Assure the continuity of data-processing services.

The following section will describe the current DoD environment intended to satisfy these three policy objectives.

## **SECTION 2. SECURITY WITHIN DOD**

Computer system security is just one aspect of DoD security. Overall security policy is specified separately for DoD elements and contractors. DoD Reg. 5200.1-R is the controlling standard for DoD elements while DoD 5220.22-M Industrial Security Manual for Safeguarding Classified Information applies to contractors.

Computer security policy-making authority is dispersed among a variety of organizations. The National Security Agency (NSA) and the National Computer Security Center (NCSC) are the primary DoD policy-making organizations. The National Institute of Standards and Technology (NIST) is the primary computer security policy-making organization for civilian Federal agencies and, in many instances, the defacto policy maker for businesses.

ADP security policy is specified in many documents. Three of the major documents for DoD Service elements are DoD Dir. 5200.28 (Security Requirements for Automated Information Systems), DoD Man. 5200.28 (ADP Security Manual), and, DoD Std. 5200.28 (Trusted Computer System Evaluation Criteria). Chapter 12 of 5220.22-M specifies ADP security requirements for contractors.

Even though there is extensive federal policy concerning ADP security, no policy firmly address certain emerging technical issues or the potential for "conflicting" interests within an industry/DoD shared-data environment. NCSC is attempting to address many of the technical issues by promulgating a series of technical computer security guidelines, commonly referred to as the "rainbow" series (due to their various cover colors).

### **2.1 System Resource Security**

Hardware, firmware, and software responsible for the protection of system resources are defined as the Trusted Computing Base (TCB). The TCB can be viewed as the security perimeter or the security relevant portion of a system. Historically, the TCB has been easy to isolate from external interactions and therefore relatively easy to protect from potential threats.

Typically the TCB has consisted of an operating system (or key operating system elements), and system files and data. In some instances, a limited set of utilities and applications were also included in the TCB. In this type of functional environment a limited set of users interacted directly with the operating system, or a limited set of utilities and applications. This type of environment is illustrated in Figure 2, with the shaded area designating the TCB.

These four layers of functionality were typically isolated in an access-controlled facility. This security was often coupled with administrative and technical restrictions that provided additional protection at a reasonable cost.

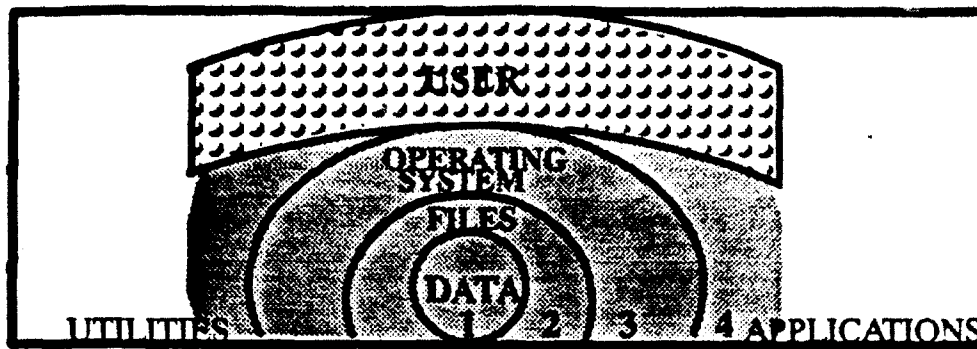


FIGURE 2. Trusted Computing Base

This geographically centralized, homogeneous TCB pictured in Figure 2 is evolving into the geographically dispersed (networked), heterogeneous set of assets pictured in Figure 3. These assets not only include existing hardware and associated software, but new classes of communications equipment and associated software. These new assets have greatly expanded the scope of the TCB.

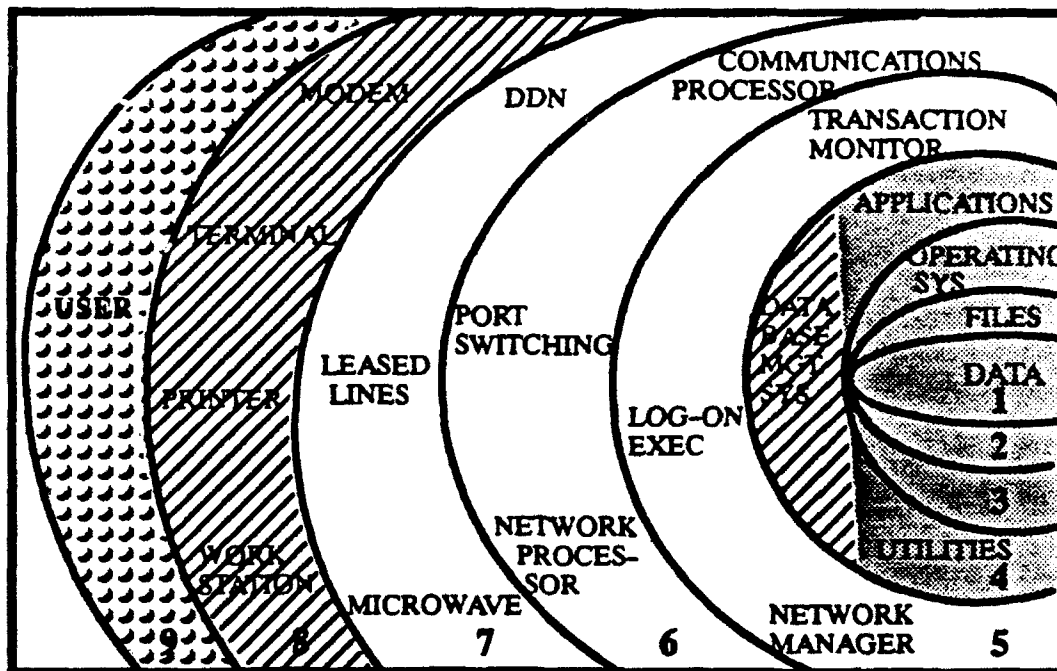


FIGURE 3. Expanded Trusted Computing Base

The expanded TCB includes nine functional layers; the original four layers (1 through 4) that originally constituted the TCB, four additional layers (5 through 8) associated with a network that formerly were excluded from the TCB, and a greatly expanded user population (9).

These nine layers require new forms of protection if the information system and its data are to remain secure. The NCSC is in the process of developing and promulgating additional technical computer security guidelines to address areas such as networking (layers 5, 6, and 7) and database management systems (a portion of layer 4).



### 2.1.1 Fundamental Computer Security Requirements

Six fundamental security requirements have been defined in DoD Std 5200.28 to evaluate security features of a TCB. These requirements are:

- **Security Policy**– An explicit, well defined set of access rules among subjects and objects that are enforced by the system.
- **Marking** – A capability to reliably label every object indicating its sensitivity level and the approved access modes.
- **Identification** – Identification and authorization information must be securely maintained for every active system element that performs some security-relevant action.
- **Accountability**– Audit information must be kept and protected so that actions affecting security can be traced.
- **Assurance** – The system must contain identifiable mechanisms that can be independently verified as enforcing requirements 1 through 4.
- **Continuous Protection** – Mechanisms that enforce basic security requirements must be continuously protected against tampering and unauthorized changes.

These six requirements are applied as criteria to evaluate the degree of protection that a TCB provides. The degree of protection is categorized in a hierarchical structure of protective mechanisms. This hierarchy is divided into four divisions:

- Division D – Minimal Protection
- Division C – Discretionary Protection
- Division B – Mandatory Protection
- Division A – Verified Protection

Each of these broad divisions signifies a major improvement in the protection afforded information in a TCB. Within Divisions B and C are a number of hierarchical subdivisions known as "classes." Classes within a division represent minor improvements in the protection afforded information in a TCB.

Currently the fundamental computer security requirements and the hierarchy of protective mechanisms reflect security control objectives for a centralized TCB. However, additional security requirements for a networked environment need to be incorporated into the fundamental computer security requirements and the protective mechanisms hierarchy described above.

### 2.1.2 Data Security and Its Classification

Three basic classification levels for data are defined in DoD Reg. 5200.1R, CONFIDENTIAL, SECRET, and TOP SECRET. These three classification levels have been expanded to

support a variety of other considerations. For example, seven levels of classification have been defined to assess information system risk.

Six levels were proposed by National Security Decision Directive (NSDD) 145 in an attempt to address concerns about the disclosure of sensitive information that, while not secret or confidential, could still jeopardize national security. Central to this concern is the fact that significant intelligence can be often surmised from a set of nonclassified items. NSDD 145 was rescinded because of civil liberties concerns. Currently there are no effective mechanisms to address this data aggregation security issue.

Also, no current DoD data classification schemes address corporate concerns for proprietary data rights. Some concerns focus on the proprietary nature of technical information (intellectual property rights and trade secrets) while others deal with possible disclosure of sensitive business/financial data. Additional standards for sharing and safeguarding different data sets among various organizations are needed.

## **2.2 Security Procedures**

Three broad categories of procedures, physical, administrative, and technical, are used to secure system resources. These categories can be further divided into protective features that include Physical Security, Procedural/Administrative Security, Personnel Security, Hardware Security, Software Security, TEMPEST Security, and Communications Security. Figure 4 illustrates how security procedures and protective features typically apply to system resources.

**Physical Security** focuses on controlling access to computer system resources. System resources must be in a controlled area if the system is processing compartmented information. Media must be controlled, labeled, stored, and handled according to the highest system classification. For networked systems, physical security deals with both decentralized processing equipment and the transmission lines and links that handle signals.

**Personnel Security** deals with the clearance of system operation/maintenance staff. All operators, analysts, and system administrators typically must be cleared to the highest level of information processed on the system. Contractor or maintenance personnel are cleared system high whenever possible. Development personnel must have at least a secret clearance.

**Procedural/Administrative Security** is typically aimed at establishing standard operating procedures (SOP) to govern access to system resources including the facility, computer equipment, media, and data/information. The SOP also often includes mandatory training of personnel, and preventive maintenance and periodic inspection of hardware.

**Hardware Security** ensures continuity of operation by the system resources, including the provision of uninterrupted power sources, incorporation of backup and restore procedures, and the incorporation of self-test capabilities in system devices.

SYSTEM RESOURCES	COMPUTER SYSTEM			NETWORK SYSTEM		
SECURITY PROCEDURES/ PROTECTIVE FEATURES	Hardware	Firmware	Software	Physical Links/Lines	Comm./ Network Software	Trans- mission Signals
PHYSICAL	●	●	●	●	●	
ADMINIS- TRATIVE						
Personnel	●	●	●	●	●	
Procedural	●		●		●	
TECHNICAL						
Hardware	●	●				
Software		●	●			
Tempest	●	●		●		
Communication				●	●	●

FIGURE 4. Application of Security Procedures to System Resources

Software Security must address the six fundamental security requirements. In addition to assuring compliance of operating systems, software security is expanding to include database management systems as well as miscellaneous utilities and customized applications. Developmental software often needs to be developed in controlled environments with cleared personnel.

TEMPEST Security involves controlling the "leakage" of electronic emanations from hardware. TEMPEST certification must be obtained before seeking accreditation. TEMPEST guidelines require that classification separation and emanation control, and their effects on equipment and its design, be discussed by all interested parties before implementation.

Communication Security protects and controls the information passing over communications channels/lines. Certification for processing information over DDN must be obtained before seeking accreditation.

Network access identification procedures, such as passwords, token based access privileges, and biometric identification, control access to the network and other system resources. Data encryption devices and schemes can also be used to control access as well as protect the confidentiality of the transmission. Public and private keys (i.e., encryption schemes) have effectively protected network access and message confidentiality. Other techniques such as sink/source unique identifiers, unique cabling design, and TEMPEST control offer additional means of maintaining data security across communication channels/lines.

## **2.3 Certification and Accreditation - Administration of System Resource Security**

Security certification is a technical evaluation of a computer system using specific security requirements as evaluation criteria. Typically, certification includes evaluation of hardware; firmware; software security design, configuration, and implementation; and supporting administrative and physical controls. Additionally, security controls for networks often need to be evaluated.

Accreditation is a management responsibility that includes acquiring of approval from the appropriate government agency to process sensitive information in a specific operational environment. Accreditation is based on a security evaluation of the system's protective features working in concert. Thus, accreditation of a system can be at a level higher than the certification of individual components. Typically this "risk" is somewhat mitigated by the implementation of additional physical and administrative controls on the operation of the computer system.

Although certification and accreditation are well-established processes, no comprehensive policy today covers the application of computer system evaluation criteria to establish computer security requirements. CSC-STD-003-85, Guidance for Applying the DoD Computer System Evaluation Criteria in Specific Environments offers recommendations for establishing the minimum acceptable security level. This standard suggests that a level of risk be established for a system. This level of risk, known as the risk index, is computed by establishing the difference between the minimum user clearance and the maximum data sensitivity. The resulting risk index is correlated to a minimum TCB security class.

### SECTION 3. SECURITY WITHIN CALS

The CALS environment is evolving from manual, paper-intensive "weapon system life cycle" processes, to a highly automated environment that depends on information technology. This evolution will occur in stages, with CALS first migrating into a data-interfaced environment, then to an environment with shared data, and finally to a functionally integrated environment.

At the simplest level, CALS integration (as pursued under CALS Phase I) refers to the interface of information among various systems. This information exchange occurs either through a physical media exchange or through interactive access of remote terminals.

A more complex level of integration, shown in Figure 8, involves data integration among the various functions and disciplines associated with weapon system acquisition and logistics. This requires the sharing of data among various organizations and sites. This integration of data into a unified set of information is the integration concept most commonly associated with CALS Phase II.

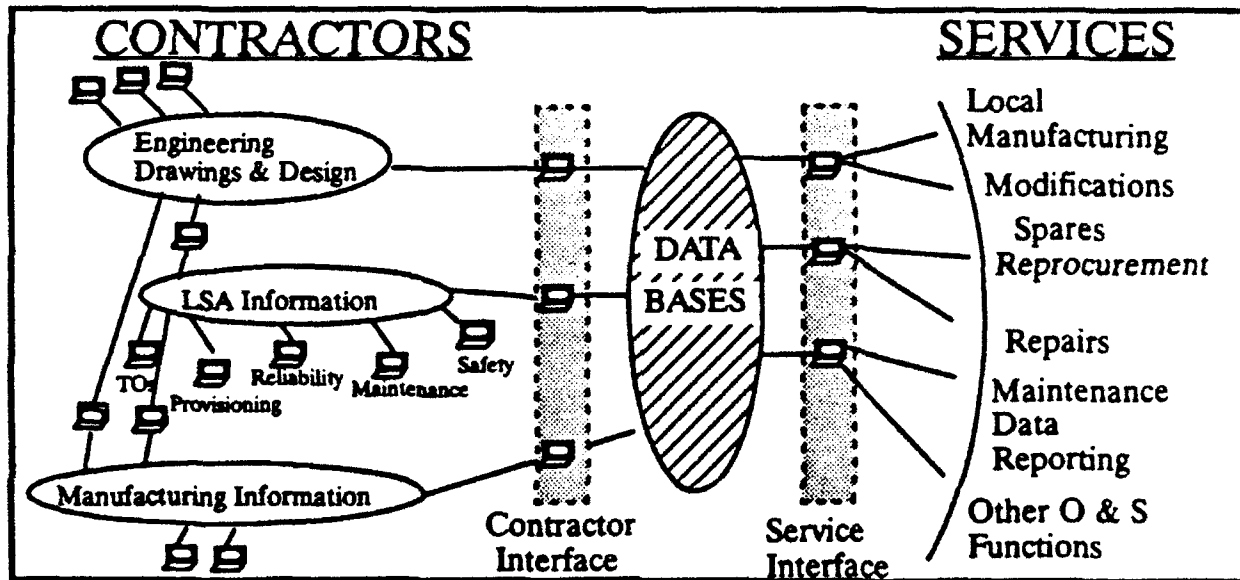


FIGURE 5. The Integrated Phase II CALS Environment

The most complex level of integration - functional integration - involves unifying functions that are currently separate activities or duplicated among various organizations. Functional integration, which necessarily includes data integration, is the most advanced integration proposal. Concepts such as concurrent engineering, where several disciplines are integrated and performed in parallel rather than sequentially, approach functional integration.

Three security risk factors accompany this evolution;

- Extensive application of information systems,

- Increased networking and remote access, and
- Technological advances resulting in resource sharing and open systems architecture.

The growing reliance on automated information systems increases potential computer security threats. Further, with an increased reliance on networking, the local "computer room" is expanding into a national and sometimes international chamber. This trend greatly expands the vulnerabilities to both human and environmental threats. Finally, technological advances that support a networking environment also provide avenues for unauthorized access to system resources as well as opportunities for the unauthorized disclosure of information. The development of an open systems architecture, in particular, greatly increases the potential of unauthorized access to system resources.

### 3.1 CALS Security - Scope of Requirements

Many security requirements are facing the CALS initiative. Although CALS affects almost all areas of information systems security, not all the affected areas are unique to CALS security and therefore are not included in the scope of this discussion.

One way to group various security areas, and thereby facilitate their organization into a relevant framework for CALS, is to define a logical security grouping and a physical security grouping. As shown in Figure 6, logical security can then be defined to include data, system, and communications security. Physical security can include computer, operations, and personnel security.

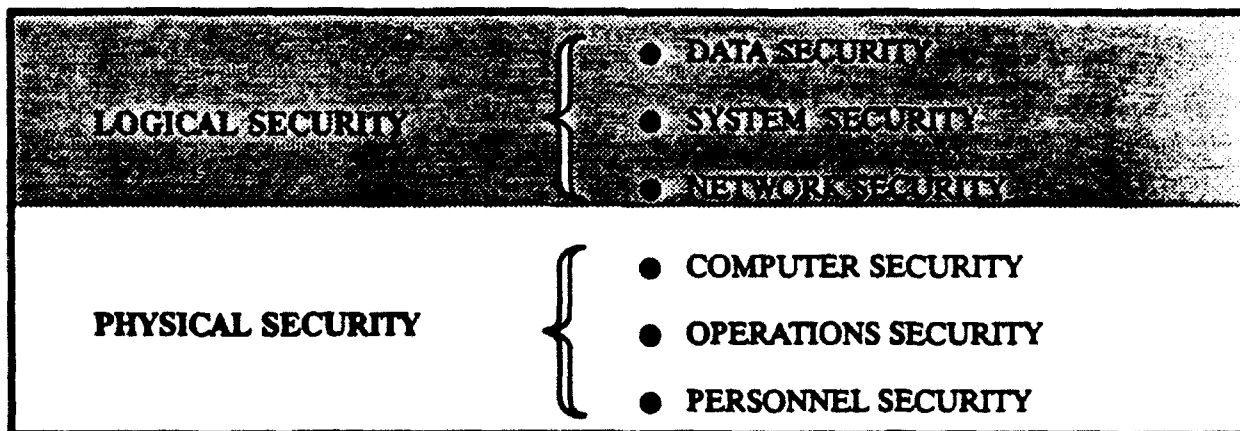


FIGURE 6. Potential CALS Security Domains

CALS Phase II presents requirements within these security domains that are in some instances new and in other instances quite problematic. Although satisfying requirements in both security domains is a necessary precondition for a successful CALS initiative, there is little that is unique within the world of CALS related to physical security. For that reason, primary interest from a CALS policy perspective must focus on the logical security domain.

Within the logical security domain, security involves two separate considerations; secrecy and integrity. Secrecy deals with the prevention of unauthorized disclosure while integrity deals with unauthorized or inadvertent modification. Computer viruses and Trojan horses are security threats involving integrity and not secrecy. Data, system, and network security must deal with both considerations to be effective.

### **3.2 Data Security Requirements**

Data security in a CALS environment presents unique challenges, ranging from controlling the access and aggregation of data into sensitive information to classifying and administering business sensitive data. These data security issues deal primarily with data secrecy. Although data accuracy, validity, and correctness is of paramount importance in any application (including CALS), the CALS environment does not introduce any unique requirements in this area.

Controlling data aggregation is a crucial requirement, currently without any technical solution. If data access/aggregation is not controlled, individual items of non-sensitive/classified information can be accessed and pieced together to present information of greater sensitivity than any one item. Much of the integration envisioned within CALS may have to be significantly curtailed without an effective means of meeting this potential threat. After an effective strategy has been developed, appropriate procedures must also be defined.

Another requirement confronting CALS is the protection of business-sensitive information. This involves protecting technical data rights among competing enterprises as well as proprietary data on cost, pricing, and other financial information. Satisfying this administrative requirement involves both the development of new data classification categories for various types of business-sensitive information and new procedures to classify the information and to administer its custody.

### **3.3 System Security Requirements**

System security may represent the greatest challenge to a CALS Phase II environment. Secrecy and integrity are both system security concerns that a successful CALS Phase II will need to satisfy. The multidimensional expansion of the TCB will affect both the functionality and scope of the system, and place unique demands upon security procedures. The first dimension of this expansion involves adding "rings of functionality" - including DBMS, communications software, network software, network configurations, and remote peripheral equipment. Expanding the number of systems linked together and therefore bringing about an associated increase in the diversity and number of users constitutes the second dimension. This growth increases exposure to unauthorized access, disruptions from occurrences such as computer viruses, and environmental threats from weather and other phenomena.

There is a wide variety of security requirements associated with an expanded TCB. Some of these requirements are associated with networks and are discussed in the next section. Other

requirements are being dealt with by the NCSC and NIST. However, there are three system security requirements that are CALS unique and need to be discussed. These are:

- Shared-data accountability,
- Risk assessment, and
- CALS certification/accreditation guidelines.

An overall approach to the management of accountability across numerous interfaced and integrated systems needs to be defined. In developing an overall approach, there are several issues that need to be addressed. One issue deals with discretionary security controls (i.e., need to know) and their application in a distributed environment. A second issue deals with the strategy used to register users. Specifically, it must be determined whether there will be one centralized user "look-up" table with authorization information or many regional/local authorization tables. A third issue concerns administrative procedures for user authorization/registration and audit.

A generic risk analysis for "CALS-like" systems also needs to be performed. This analysis should be coordinated with the appropriate designated approving authorities (DAAs). The analysis should identify the type of threats that different CALS-like systems will face, estimate the nature and probability of potential losses, and identify an array of appropriate remedial measures that may be employed to reduce potential losses and mitigate potential threats.

The third requirement deals with the need to provide the Services with guidelines concerning security certification and accreditation. Currently, no concrete guidance exists concerning accrediting decentralized systems. Current guidelines are unclear when a decentralized system should be accredited as a series of separate information systems and when it should be accredited as a unified whole. In addition, no guidance exists concerning the preferred manner in dealing with different levels of classified information and various user clearances. Without clear guidelines, physical separation of information may be the preferred solution. This solution will defeat CALS's major objective, which is integration. Just as the CALS initiative has developed a program implementation guide, some sort of security guide to risks, certification and accreditation, and security procedures needs to be developed and provided to the Services.

### **3.4 Network Security Requirements**

Network integrity is the third domain critical to the envisioned CALS Phase II environment. Phase II projects will rely on data integration, remote access over communication lines, and a variety of network services. Although efforts for several years have focused on establishing network security requirements for these services, to date there is little official policy within DoD applicable for the establishment of project security guidelines.

Network security requirements, although not unique to CALS, are crucial enablers for CALS Phase II. Three areas of primary importance are:



- Communications Security {
  - Origination Authentication
  - Field Integrity
  - Message Nonrepudiation
- Compromise Protection {
  - Data Confidentiality
  - Traffic Confidentiality
  - Routing Flexibility
- Network Management {
  - Denial of Service Protection
  - Diagnostic Services

Communications security involves three related issues. First, there is a need to be able to assure the origination of a remote message/request. Second, there is a need to assure that any or all fields in a data stream are not changed, either intentionally or unintentionally. The third need is to be able to prove that: 1) a data stream was sent to a location, and 2) that the data stream was received at a location. This nonrepudiation characteristic is critical in attaining confidence in remote transaction processing.

Compromise protection, a second requirement area, assures that messages are not disclosed to unauthorized parties. This requirement has three conditions that must be satisfied: data confidentiality must be protected; traffic confidentiality must be protected; and users must have flexibility in selecting the route of their message as an added assurance to both data and traffic confidentiality.

Although requirements for communications security and compromise protection have not been formally established, various encryption schemes, including public and private keys, address many of the needs discussed above. If it is determined that these requirements are crucial, encryption schemes may need to be devised for CALS and associated administration procedures developed. The administration of keys on a national scale for CALS may create issues that require special consideration.

Technical requirements to effectively manage a network constitute the third area of concern. Within this area, requirements must be defined to assure user protection from denial of service (DOS). Levels of DOS protection/assurance also need to be defined. Additionally, various diagnostic services (e.g., network use, routing availability) also need defining.

The final requirement, more administrative in nature, involves incorporating the above referenced network service requirements into the security hierarchy defined in the Trusted Computer System Evaluation Criteria. Each division, and classes within each division, should be associated with specific services. In some instances, distinctions must be made for a service requirement based on its strength. This type of guidance will be needed to implement Phase II CALS.

### 3.5 CALS Security Requirements – Summary

CALS security requirements are either technical or administrative in nature. Technical requirements typically need research and development to define solutions in areas that represent potential threats. Administrative requirements deal primarily with the need to update/enhance security policies that are reflected in standards, manuals, and circulars.

Although there are a multitude of security requirements facing CALS, interest needs to be focused on those that are unique to CALS. Figure 7 lists those requirements that are CALS-unique in the sense that their solution needs to be tailored to CALS.

	TECHNICAL	ADMINISTRATIVE
DATA SECURITY	<ul style="list-style-type: none"> <li>• Data Aggregation Protection Schemes</li> </ul>	<ul style="list-style-type: none"> <li>• Classification levels for sensitive business information</li> <li>• Procedures to classify and administer business data</li> </ul>
SYSTEM SECURITY	<ul style="list-style-type: none"> <li>• Shared Data Accountability Procedures</li> <li>• Risk Assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Certification/Accreditation Guidelines for CALS Systems               <ul style="list-style-type: none"> <li>– Protection Philosophy</li> <li>– Implementation Strategy</li> </ul> </li> </ul>
NETWORK SECURITY	<ul style="list-style-type: none"> <li>• Data Encryption Scheme</li> </ul>	<ul style="list-style-type: none"> <li>• National Key Management Procedures</li> </ul>

FIGURE 7. CALS Security Requirements

The network security requirements shown in Figure 7 do not adequately satisfy the needs of CALS. However, the other requirements discussed in Section 3.4 are in no way unique to CALS. Therefore it is crucial for the CALS program to maintain an awareness of developments in this area, and, where feasible, work with NCSC in defining those requirements.

## **SECTION 4. RECOMMENDATIONS**

Developing and executing a well-thought-out security policy is critical for a successful CALS. While not an enabling technology, security is critical because it is a "disabling technology" that must be satisfied in order to integrate. Adequate security plans will help expedite the integration of technology, organizations, functions, and data envisioned as part of CALS.

Specific goals, such as those listed below, need to be focused on to assure their attainment.

- Specify security policy and requirements for new acquisitions and technology vendors.

Security requirements must be specified and agreed upon quickly to provide guidance to new weapon system acquisitions as well as to technology vendors. As described in the previous section, the CALS initiative needs to address some critical issues. The manner in which these issues are addressed may affect tomorrow's hardware and software.

- Integrate security considerations early-on into CALS architectural concepts.

Security considerations need to be incorporated into emerging CALS system architectural concepts. Just as there are critical activities in the acquisition life cycle for a weapon system or information system, security also has a set of life cycle activities. If security is not incorporated into initial CALS architectural concepts, security requirements may later constrain design, development, and operations.

- Provide a standard to assess the adequacy of security measures for ongoing CALS efforts.

Security guidance is needed by ongoing CALS infrastructure projects and technology demonstrations. Although these projects are at various life cycle stages, specific guidance on security can still be incorporated into some of these projects. In other instances, such guidance will provide input to follow-on or enhancement efforts.

### **4.1 CALS Security Initiative - A Strategic Approach**

CALS is facing a variety of requirements in the security area. If the CALS program were to attempt to satisfy all of these requirements, large amounts of manpower and funding would have to be committed. Therefore, OSD needs to leverage the activities of other organizations and only undertake those activities that target satisfying CALS unique requirements.

Specifically, OSD needs to develop an overall policy for CALS-related activities, and develop high-level conceptual models in support of CALS operating concepts and implementation strategies. Organizations such as NCSC, NSA, and NIST will need to continue to examine some of the technical issues confronting the security community and establish the

### **Define security concept of operations including scope of CALS security interest**

This task involves identifying the various operational scenarios associated with both Phase I and Phase II concepts. For each type of digital deliverable acquisition, a broad operating concept will need to be developed and potential risks identified. In addition, various Phase II integration architectures/concepts will also need to be defined and associated with potential threats and risks.

### **Develop appropriate protection philosophies and identify appropriate risk management mechanisms for CALS**

Based on the operational scenarios defined in Task 1, upper level protection philosophies need to be defined. Initial focus should be on strategies to handle multiple levels of classified information and on strategies to protect distributed systems. Once top level strategies are developed, specific mechanisms and security procedures can be conceived to address specific application requirements.

### **Initiate discussions on certification/accreditation with appropriate designated approval authority(s) (DAAs)**

As risk management mechanisms are being identified, appropriate DAAs will need to be identified. Discussions will focus on accreditation of potential CALS applications. These preliminary discussions may lead to revised direction or validate the approaches proposed to manage risks.

### **Develop implementation strategies for CALS security requirements**

A result of the above tasks will be the identification of items or requirements that are on the critical path of CALS. Based on that assessment, an overall implementation strategy can be developed. This strategy would include specific output requirements associated with dates and organizational responsibilities.